

# **Отчёт по лабораторной работе №1**

**Шифры простой замены**

Левкович Константин Анатольевич

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Задание</b>	<b>6</b>
<b>3</b>	<b>Теоретическое введение</b>	<b>7</b>
<b>4</b>	<b>Выполнение лабораторной работы</b>	<b>9</b>
<b>5</b>	<b>Выводы</b>	<b>11</b>

## Список иллюстраций

3.1	Стандартная реализация Шифра Цезаря (сдвиг на 3) . . . . .	7
3.2	Шифр Атбаш . . . . .	8
4.1	Программная реализация шифра Цезаря . . . . .	9
4.2	Программная реализация шифра Атбаш . . . . .	10
4.3	Вывод программы . . . . .	10

## Список таблиц

# 1 Цель работы

Ознакомиться с шифрами простой замены: шифр Цезаря и шифр Атбаш.  
Реализовать шифры программно.

## 2 Задание

- Реализовать шифр Цезаря с произвольным ключом  $k$ ;
- Реализовать шифр Атбаша.

### 3 Теоретическое введение

В основе функционирования цифров простой замены лежит следующий принцип: для получения шифртекста отдельные символы или группы символов исходного алфавита заменяются символами или группами символов шифроалфавита.

Шифр Цезаря является примером метода подстановки. Он является моноалфавитной подстановкой, то есть каждой букве открытого текста ставится в соответствие одна буква шифртекста. В оригинальной шифре Цезаря используется сдвиг на три символа. Обобщенный вид шифра Цезаря предполагает сдвиг символов на произвольное число  $k$ . Для стандартного алфавита математический вид шифра принимает вид: позиции символа в шифроалфавите есть остаток от деления на кол-во символов в алфавите (26) от позиции символа в исходном алфавите вместе со сдвигом  $k$ .

$$E_n(x) = (i + k) \bmod 26$$

,

где  $i$  - значение открытого текста,  $k$  - номер сдвига.

Шифр Цезаря со сдвигом 1 (рис. 3.1):

ABCDEF GHI J KLMNOPQRSTUVWXYZ  
DEFGHI J KLMNOPQRSTUVWXYZABC

Рис. 3.1: Стандартная реализация Шифра Цезаря (сдвиг на 3)

Шифр Атбаш - шифр простой замены со сдвигом на всю длину алфавита. Для

алфавита, состоящего только из русских букв и пробела, таблица шифрования будет иметь следующий вид: (рис. 3.2):

а б в г д е ж з и й к л м н о п р с т у ф х ц ч ш щ ъ ы ь э ю я \_  
\_ я ю э ь ы ъ щ ч ц х ф у т с р п о н м л к й и з ж е д г в б а

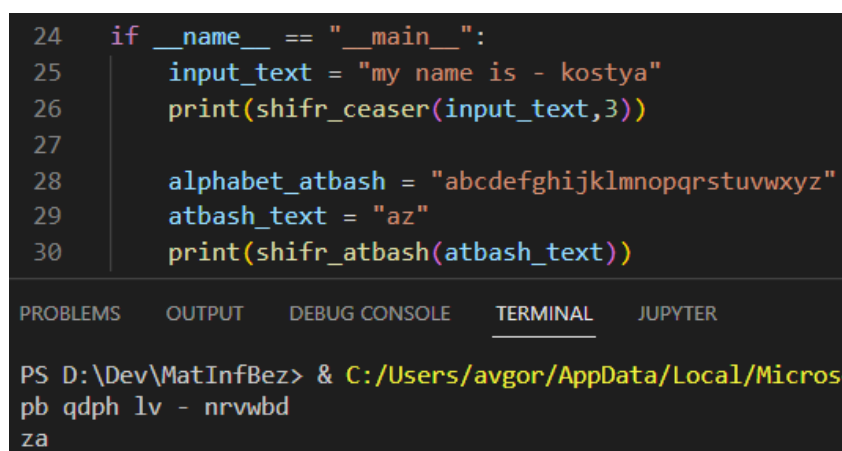
Рис. 3.2: Шифр Атбаш



## 4 Выполнение лабораторной работы

Работа была выполнена на языке программирования Python.

Сначала реализуем шифр Цезаря (рис. 4.1):



```
24 if __name__ == "__main__":
25     input_text = "my name is - kostya"
26     print(shifr_caesar(input_text,3))
27
28     alphabet_atbash = "abcdefghijklmnopqrstuvwxyz"
29     atbash_text = "az"
30     print(shifr_atbash(atbash_text))
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL JUPYTER

```
PS D:\Dev\MatInfBez> & C:/Users/avgor/AppData/Local/Micros
pb qdph lv - nrwbd
za
```

Рис. 4.1: Программная реализация шифра Цезаря

Задаем алфавит `alphabet`, состоящий из латинских букв нижнего регистра. Функция `shifr_caesar` принимает на вход 2 аргумента: `input_text` - входное сообщение, необходимое зашифровать и `k` - сдвиг алфавита. В цикле для каждого символа проверяется вхождение в исходный алфавит. Для непопавших в алфавит символов замены не требуется, так как сюда попадают спецсимволы. Если символ встретился в алфавите, то из исходного алфавита берется символ, соответствующий остатку от деления на 26 исходного символа, сдвинутого на `k`.

Реализация шифра Атбаш (рис. 4.2):

```
def shifr_atbash(input_text, alphabet="abcdefghijklmnopqrstuvwxyz"):
    output_text = ""
    len_alp = len(alphabet)
    for char in input_text:
        if char in alphabet:
            output_text += alphabet[len_alp - alphabet.index(char)-1]
        else:
            output_text += char
    return output_text
```

Рис. 4.2: Программная реализация шифра Атбаш

Функция `shifr_atbash` принимает на вход открытый текст и алфавит. По умолчанию значение алфавита будут латинские буквы нижнего регистра. Логика для спецсимволов данного шифрования аналогична шифру Цезаря: они не изменяются и попадают в зашифрованное сообщение в исходном виде. Для всех других символов берется зеркально отраженный символ из алфавита: — — 1.

Программная реализация шифров Цезаря и Атбаш представлена на рисунке: в обе функции подается один обязательный аргумент - открытый текст и необязательный. Для шифра Цезаря задается сдвиг, для шифра Атбаша задается произвольный алфавит. (рис. 4.3):

```
24 if __name__ == "__main__":
25     input_text = "my name is - kostya"
26     print(shifr_ceaser(input_text,3))
27
28     alphabet_atbash = "abcdefghijklmnopqrstuvwxyz"
29     atbash_text = "az"
30     print(shifr_atbash(atbash_text))
```

ПРОБЛЕМЫ    ВЫХОДНЫЕ ДАННЫЕ    КОНСОЛЬ ОТЛАДКИ    ТЕРМИНАЛ    ЛУ

```
PS D:\Dev\MatInfBez\lab1> & C:/Users/avgor/AppData/Local/M
pb qdph lv - nrwvbd
za
```

Рис. 4.3: Вывод программы

## 5 Выводы

Ознакомился с шифрами простой замены: шифр Цезаря и шифр Атбаш.  
Реализовал шифры программно на языке программирования Python.